Bloomberg BNA

Telecommunications Law Resource Center

Privacy Regulation on the Internet

Although Internet Service Providers (ISPs) are not the only entities with access to consumers' electronic data, and despite the fact that ISPs are already subject to a higher level of privacy regulation than other companies, the Federal Communications Commission plans to impose additional privacy regulations on ISPs, and ISPs alone. The author suggests that an even-handed regulatory regime is necessary and proper, and further suggests that the Federal Trade Commission, with its deeper experience in the realm of consumer privacy protection, is better suited then the FCC to the task of imposing it.

Level the Privacy Playing Field to Protect Consumers

BY RICK BOUCHER

Privacy in our digital world is once again making headlines, from the controversy over unlocking Apple's encryption system to the latest breaches of information from e-commerce providers. Lost in all of this discussion—though also illuminated by it—is a tectonic shift in who has access to a user's electronic data, a change that has profound implications for how privacy should be protected in the future.

Start from a simple point, with which users of digital devices would likely agree: All participants in the Internet economy should extend similar privacy protections to users. That only seems fair. The Internet user's most important interest, after all, is to have confidence that his or her privacy is being uniformly protected throughout the Internet ecosystem by all entities that have access to users' information.

Rick Boucher was a member of the US House for 28 years and chaired the House Energy and Commerce Committee's Subcommittee on Communications and the Internet. He is honorary chairman of the Internet Innovation Alliance (IIA) and head of the government strategies practice at the law firm Sidley Austin.

What Can an ISP See? There is a common misperception, dating from the early days of the ''information superhighway,'' that Internet Service Providers (ISPs) have access to all information that a consumer either sends or receives via the Internet. But a misperception it is, in two ways.

First, broadband providers are subject to the privacy requirements of Section 222 of the Communications Act of 1934, as amended (added by Section 702 of the Telecommunications Act of 1996), which addresses Consumer Proprietary Network Information (CPNI). In reality, therefore, ISPs are just companies that connect users to the Internet with a sharply limited and rapidly declining ability to look into the content for which consumers search and transmit over their networks.

In addition, a number of fundamental changes in the way consumers access the Internet – particularly the escalating use of strong encryption, the switch to mobile access, the use of multiple devices, and the rise of both Wi-Fi and private networks – give other types of companies, rather than traditional ISPs, powerful tools to see into consumers' Internet usage.

Where, then, should the new focus be in protecting consumer privacy? A recent paper from Peter Swire of Georgia Tech illustrates the differences between ISPs and other companies, and it should have a direct bearing on decisions regarding the protection of consumer privacy. As Swire concludes, ''ISPs have neither com-

prehensive nor unique access to information about users' online activity. Rather, the most commercially valuable information about online users . . . is coming from other contexts.'' Secure encryption protocols like HTTPS, which already accounts for 49 percent of Internet traffic, do not permit ''deep packet inspection'' of data. An ISP only routes the packets and has no opportunity to determine their content; ISPs cannot even see a search query or full URL in HTTPS. The study estimates that, by the end of this year, 70 percent of Internet traffic will be encrypted and beyond the surveillance of ISPs. And it's the same with Internet video, where only the website hosting the content gains data insights about users. Nevertheless, the study clearly shows that edge providers like Facebook and Google, as well as major e-commerce sites, have more opportunity to surveil content than ISPs, giving them unique insights into user activity.

Who Gets Regulated, and By Whom? Would it then be a surprise to hear that the Federal Communications Commission (FCC) is readying a proposal to impose new privacy rules on ISPs that would not apply to these other Internet entities?

In today's world, single wireline Internet-connected devices in consumers' homes account for a rapidly declining share of Internet traffic. Nearly half (46 percent) of traffic travels over Wi-Fi networks outside the home, a number that will grow to 60 percent by 2020. And non-ISPs dominate platforms that track users across devices (e.g., social media) and account for most Internet advertising. As we have seen in the recent Apple encryption controversy, the mobile operating system (iOS or Android) facilitates collection of location data. It's also highly correlated with advertising. The wireless carrier, an ISP, is not situated to undertake any of this data collection.

The implications of Swire's paper are clear: Information that consumers send and receive over the Internet is subject to widely imbalanced privacy protections (in some instances, basically none at all) every time information changes hands. For example, even though ISPs do not have visibility into most data crossing their networks, the privacy regulations imposed on them under existing CPNI regulations are more prescriptive than the privacy protection obligations required of edge providers, which have essentially unbridled access to information about consumers who use their websites. This dichotomy makes no sense – and the problems of disparate privacy regulation become only more profound as we move towards the hyper-connected Internet of Things.

Unifying Internet privacy protections under a single agency would better ensure equal treatment of consumer data by all participants in the Internet ecosystem. To unify regulation, it would make sense for Congress to choose the agency with the greatest breadth of experience and institutional knowledge in the area. Given its long history of work in consumer protection generally and privacy protection in particular, the Federal Trade Commission is a better choice than the FCC. Uniformity of privacy assurances overseen by a single expert agency is the best way to give consumers peace of mind as they surf the Web to shop, work and learn in today's digital world.

  ISSN